



# FortiAnalyzer - Release Notes

VERSION 5.4.2

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



February 23, 2016

FortiAnalyzer - Release Notes

05-542-393213-20170223

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Supported models	6
What's new in FortiAnalyzer version 5.4.2	7
Security Service—Indicators of Compromise	7
FortiView	7
Reports	7
Event Management	7
Log View	8
System Settings	8
Product Integration	8
Help	8
<b>Special Notices</b>	<b>9</b>
Hyper-V FortiAnalyzer-VM running on an AMD CPU	9
IPsec connection to FortiOS for logging	9
Datasets Related to Browse Time	9
System Configuration or VM License is Lost after Upgrade	9
SSLv3 on FortiAnalyzer-VM64-AWS	10
No support for remote SQL database	10
Pre-processing logic of ebtime	10
Log Aggregation or Forwarding	10
<b>Upgrade Information</b>	<b>11</b>
Upgrading to FortiAnalyzer 5.4.2	11
Downgrading to previous versions	11
Firmware image checksums	11
FortiAnalyzer VM firmware	11
SNMP MIB files	13
<b>Product Integration and Support</b>	<b>14</b>
FortiAnalyzer version 5.4.2 support	14
Feature support	15
FortiGate Management	16
Language support	17
Supported models	18

**Resolved Issues ..... 25**

Device Manager ..... 25

FortiView ..... 25

Logging ..... 26

Reporting ..... 26

System Settings ..... 27

Others ..... 27

Common Vulnerabilities and Exposures ..... 27

**Known Issues ..... 29**

FortiView ..... 29

Logging ..... 29

Reporting ..... 29

System Settings ..... 29

## Change Log

Date	Change Description
2016-12-14	Initial release of 5.4.2.
2016-12-15	Added 400028 to Known Issues and 389255 and 383563 to Resolved Issues. Noted that FortiAnalyzer supports Microsoft Hyper-V 2016 in the FortiAnalyzer VM Firmware section.
2016-12-21	Added support for FortiOS 5.4.3.
2016-12-29	Added special notice about Hyper-V FortiAnalyzer-VM running on an AMD CPU.
2017-01-06	Removed support for FortiOS/FortiOS Carrier 4.3.2 to 4.3.18.
2017-02-23	Added support for FortiOS 5.4.4.

# Introduction

This document provides the following information for FortiAnalyzer version 5.4.2 build 1151:

- [Supported models](#)
- [What's new in FortiAnalyzer version 5.4.2](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide*.

## Supported models

FortiAnalyzer version 5.4.2 supports the following models:

<b>FortiAnalyzer</b>	FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

## What's new in FortiAnalyzer version 5.4.2

The following is a list of new features and enhancements in FortiAnalyzer version 5.4.2.

### Security Service—Indicators of Compromise

#### IOC Enhancement

Improved threat catch rate

### FortiView

#### FortiView improvements

- Improved filters, refresh interval selection and summary headers on drilldown
- Performance improvements
- Device-level hcache now supported in FortiView

### Reports

#### SAAS Application Report

Default report template for monitoring sanctioned and unsanctioned SAAS applications

#### Cyber Threat Assessment Report

New report template for cyber threat assessment

#### Report Usability Improvements

- Simplified template configuration
- Streamlined report workflow

### Event Management

#### Events Calendar View

Displays alerts on calendar with weekly/monthly views for quick access and intuitive event monitoring

## Log View

### Add CVE-ID to Log View

Common Vulnerabilities and Exposures number (CVE ID) for known security threats added to *Log View > Security > Intrusion Prevention*

## System Settings

### Dashboard

New widget for collector mode to monitor log forwarding rate

## Product Integration

Support for FortiAuthenticator integration

## Help

Links to how-to videos in the *Help* menu



# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.4.2.

## Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## IPsec connection to FortiOS for logging

FortiAnalyzer 5.4.2 no longer supports an IPsec connection with FortiOS 5.0/5.2. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiAnalyzer. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

FortiAnalyzer 5.4.1 and earlier does support IPsec connection with FortiOS 5.0/5.2.

## Datasets Related to Browse Time

FortiAnalyzer 5.4.2 contains enhancements to calculating the estimated browse time. Due to the changes, cloned datasets that query for browse time may not be able to return any results after upgrade.

## System Configuration or VM License is Lost after Upgrade

When upgrading FortiAnalyzer from 5.4.0 or 5.4.1 to 5.4.2, it is imperative to reboot the unit before installing the 5.4.2 firmware image. Please see the *FortiAnalyzer Upgrade Guide* for details about upgrading. Otherwise, FortiAnalyzer may lose system configuration or VM license after upgrade. There are two options to recover the FortiAnalyzer unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

## SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

## No support for remote SQL database

Starting with FortiAnalyzer software versions 5.0.7 and 5.2.0, remote SQL database support will only cover the insertion of log data into the remote MySQL database. Historical log search and reporting capabilities, which rely on the remote SQL data, will no longer be supported.

Those wishing to use the full set of FortiAnalyzer features are encouraged to switch as soon as possible to storing SQL data locally on the FortiAnalyzer. The local database can be built based upon existing raw logs already stored on the FortiAnalyzer.

## Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of 13 or 2, when `logid == 13`, `hostname` must not be empty. The `service` field should be either HTTP, 80/TCP or 443/TCP.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

In version 5.0.5 or later, Explicit Proxy logs (`logid=10`) are checked when calculating the estimated browsing time.

## Log Aggregation or Forwarding

Log aggregation or forwarding works from 5.4 to 5.4 or 5.4.1 to 5.4.1. Please use the same FortiAnalyzer version on all the units. Other FortiAnalyzer versions not supported.

# Upgrade Information

## Upgrading to FortiAnalyzer 5.4.2

You can upgrade FortiAnalyzer 5.2.0 or later directly to 5.4.2. If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiAnalyzer 5.2 first. (We recommend that you upgrade to 5.2.9, the latest version of FortiAnalyzer 5.2.)



For details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide*.

---

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

### Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

### Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

### Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

### Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

### Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

### VMware ESX/ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtual-security-management.html>. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

# Product Integration and Support

## FortiAnalyzer version 5.4.2 support

The following table lists FortiAnalyzer version 5.4.2 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11</li><li>• Mozilla Firefox version 50</li><li>• Google Chrome version 54</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 5.4.0 to 5.4.4</li><li>• 5.2.0 to 5.2.10</li><li>• 5.0.4 to 5.0.12</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 5.4.0 to 5.4.2</li><li>• 5.2.0 to 5.2.9</li><li>• 5.0.0 to 5.0.13</li></ul>
<b>FortiCache</b>	<ul style="list-style-type: none"><li>• 4.1.3</li><li>• 4.0.4</li></ul>
<b>FortiClient</b>	<ul style="list-style-type: none"><li>• 5.2.0 and later</li><li>• 5.0.4 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• 5.3.8</li><li>• 5.2.9</li><li>• 5.1.6</li><li>• 5.0.10</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 5.4.0 to 5.4.2</li><li>• 5.2.0 and later</li><li>• 5.0.0 and later</li></ul>

<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>• 2.3.2</li> <li>• 2.2.2</li> <li>• 2.1.3</li> <li>• 2.0.3</li> <li>• 1.4.0 and later</li> <li>• 1.3.0</li> <li>• 1.2.0 and 1.2.3</li> </ul>
<b>FortiSwitch ATCA</b>	<ul style="list-style-type: none"> <li>• 5.0.0 and later</li> <li>• 4.3.0 and later</li> <li>• 4.2.0 and later</li> </ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"> <li>• 5.6.0</li> <li>• 5.5.4</li> <li>• 5.4.1</li> <li>• 5.3.8</li> <li>• 5.2.4</li> <li>• 5.1.4</li> <li>• 5.0.6</li> </ul>
<b>FortiDDoS</b>	<ul style="list-style-type: none"> <li>• 4.2.3</li> <li>• 4.1.12</li> </ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"> <li>• 4.2.0</li> </ul>
<b>Virtualization</b>	<ul style="list-style-type: none"> <li>• Amazon Web Service AMI, Amazon EC2, Amazon EBS</li> <li>• Citrix XenServer 6.2</li> <li>• Linux KVM Redhat 6.5</li> <li>• Microsoft Azure</li> <li>• Microsoft Hyper-V Server 2008 R2, 2012 &amp; 2012 R2</li> <li>• OpenSource XenServer 4.2.5</li> <li>• VMware: <ul style="list-style-type: none"> <li>• ESX versions 4.0 and 4.1</li> <li>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0</li> </ul> </li> </ul>



Always review the Release Notes of the supported platform firmware version before upgrading your device.

## Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	

## FortiGate Management

You can enable FortiManager features on some FortiAnalyzer models. FortiAnalyzer models with FortiManager features enabled can manage a small number of FortiGate devices, and all but a few FortiManager features are enabled on FortiAnalyzer. The following table lists the supported modules for FortiAnalyzer with FortiManager Features enabled:

FortiManager Management Modules	FortiAnalyzer with FortiManager Features Enabled
Device Manager	✓
Policy & Objects	✓
AP Manager	✓



FortiManager Management Modules	FortiAnalyzer with FortiManager Features Enabled
FortiClient Manager	✓
VPN Manager	✓
FortiGuard	
FortiMeter	
FGT-VM License Activation	

## Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
<password> <file name>
```

```
execute sql-report import-lang <language name> <sftp <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiAnalyzer CLI Reference*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.4.2. Please ensure that the log devices are supported before completing the upgrade.

### FortiGate models

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-101E, FG-140D, FG-140D-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FG-400D, FG-500D, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-2000E, FG-2500E, FG-3800D, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6  <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D  <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC  <b>FortiGate Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC  <b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM  <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager  <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
<b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-800D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B  <b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C  <b>FortiGate DC:</b> FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FGT-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC  <b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC  <b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D  <b>FortiGate Rugged:</b> FGR-60D, FGR-100C  <b>FortiGate VM:</b> FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN  <b>FortiSwitch:</b> FS-5203B, FCT-5902D	5.2

Model	Firmware Version
<p><b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B</p> <p><b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p><b>FortiGate DC:</b> FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p> <p><b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p> <p><b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate Rugged:</b> FGR-60D, FGR-90D, FGR-100C</p> <p><b>FortiGateVoice:</b> FGV-40D2, FGV-70D4</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p><b>FortiSwitch:</b> FS-5203B</p>	5.0

**FortiCarrier Models**

Model	Firmware Version
<b>FortiCarrier:</b> FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C  <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC  <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
<b>FortiCarrier:</b> FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D  <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC  <b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC  <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-VM64-XEN, FCR-VM64-AWSONDEMAND	5.2
<b>FortiCarrier:</b> FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C  <b>FortiCarrier DC:</b> FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC  <b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC  <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64	5.0

**FortiDDoS models**

Model	Firmware Version
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B	4.2, 4.1, 4.0

**FortiAnalyzer models**

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.  <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B  <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B  <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

**FortiMail models**

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B  <b>FortiMail Low Encryption:</b> FE-3000C-LENC  <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B  <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B  <b>FortiMail VM:</b> FE-VM64	5.1.6
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B  <b>FortiMail VM:</b> FE-VM64	5.0.10

**FortiSandbox models**

Model	Firmware Version
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.3.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.0 2.1.0
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.0 1.4.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

**FortiSwitch ACTA models**

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

**FortiWeb models**

Model	Firmware Version
<b>FortiWeb:</b> FWB-2000E	5.6.0
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3

Model	Firmware Version
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E  <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E  <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.8
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E  <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

#### FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E  <b>FortiCache VM:</b> FCH-VM64	4.0



# Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.4.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
382383	When there are many unregistered devices, they may intermittently disconnect from FortiAnalyzer.
382811	FortiAnalyzer should be able to sustain stable connections with more than 3500 devices and able to receive logs successfully.
306276	FortiCarrier ADOM should not be displayed when no device is registered.

## FortiView

Bug ID	Description
217103	FortiAnalyzer should allow users to view or download the Application Control archive files.
233869	There should be an option to clear search history.
371773	There may be performance issues to view logs when using the scroll bar.
379612	The filter, [-msg="Virtual cluster's vdom is added"], should display the relevant logs in the Log View.
379977	FortiAnalyzer cannot filter out users for SSL & Dialup IPSec VPNs.
382557	Drop box may become too narrow to view and select FortiGate device.
386279	Users need to click on the Go button twice before the log time frame is updated.
308171	Aggregated Dialed Time is incorrectly calculated in VPN-Top-Dial-Up and VPN-Users-By-Duration datasets.
387209	FortiGate devices that query FortiGuard should not be flagged as highly suspicious.
390173	FortiAnalyzer is unable to display part of the DLP content.

Bug ID	Description
395191	UTM Deny logs are displayed with no action on FortiAnalyzer's GUI.
397036	FortiAnalyzer should accept more characters for log view and policy search.

## Logging

Bug ID	Description
373262	FortiAnalyzer should allow users to specify the invoke time to auto delete logs.
381559	HA device logs are not received in aggregation mode.
383238	FortiAnalyzer should increase the limit for the number of aggregated clients.
393615	When using wildcard in the second or third octet for source IP in the <i>Log View</i> filter, incorrect results are returned.

## Reporting

Bug ID	Description
248563	Within the WiFi Network Summary report, AP Name should be the FortiAP's name instead of the VAP interface's name.
373718	Reports show devices with their serial numbers instead of hostnames.
377589	Blocked sites should not be counted within the Top 50 Site By Browsing Time.
383251	Reports may not contain any user data when a user filter is applied.
234007	Estimated browsing time dataset should pull log data according to time period specified.
383955	GUI fails to display chart library if there is a chart with invalid table columns.
397822	Users may not be able to generate custom reports after resizing FAZ-VM disk and rebuilding DB.
391482	User changes on LDAP server may not get updated on FortiAnalyzer for the user filter in reports.

## System Settings

Bug ID	Description
386865	Sorting for Analytics or Archive does not work on the Storage Info page.
391076	Qmail server is rejecting Email from FortiAnalyzer as the mail body contains bare LFs.
366224	FortiAnalyzer generates invalid Event logs on auto deleting policy from ADOM.

## Others

Bug ID	Description
365639	The XML call to <code>searchFazLog</code> does not return the pktlog information.
366332	Logs are not imported when there are more than 1000 log files.
376758	FortiAnalyzer needs a diagnostic command to show supported platforms.
388071	FortiAnalyzer may not be able to render a proper web GUI page when making a change.
389137	Port 8900 and 8901 may be open without being in use.
391900	Scheduled log ftp backup may not be successful.

## Common Vulnerabilities and Exposures

Bug ID	Description
384180	FortiAnalyzer 5.4.2 is no longer vulnerable to the following TMP Reference: <ul style="list-style-type: none"><li>• 2016-0023</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.
380634	FortiAnalyzer 5.4.2 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none"><li>• 2016-5387</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

Bug ID	Description
389255	FortiAnalyzer 5.4.2 is no longer vulnerable to the following CVE-References: <ul style="list-style-type: none"><li>• 2016-6308</li><li>• 2016-6307</li><li>• 2016-6306</li><li>• 2016-6305</li><li>• 2016-6304</li><li>• 2016-6303</li><li>• 2016-6302</li><li>• 2016-2183</li><li>• 2016-2182</li><li>• 2016-2181</li><li>• 2016-2179</li><li>• 2016-2178</li><li>• 2016-2177</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.
383563	FortiAnalyzer 5.4.2 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none"><li>• 2016-5696</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

# Known Issues

The following issues have been identified in FortiAnalyzer version 5.4.2. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## FortiView

Bug ID	Description
396699	Filter should be persistent when changing view from formatted log to raw log or vice versa.

## Logging

Bug ID	Description
388185	Log files for Router should include IP addresses for sites that have multiple addresses.
389592	Filter does not return any results if message is part of the filter.
400028	Policy UUID is not inserted into SQL DB

## Reporting

Bug ID	Description
390502	FortiAnalyzer should allow cloning of the pre-defined reports: <i>User Top 500 Websites by Bandwidth</i> and <i>User Top 500 Websites by Session</i> .

## System Settings

Bug ID	Description
395243	FortiAnalyzer should correctly show the local user and radius wildcard user who is performing delete, download, or import log file actions from <i>Log Browse</i> .
396417	Test Emails fails when the recipient has a different domain than the account configured under SMTP server settings.



**FORTINET®**

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.